REMARKS

Claims 4 to 6 are now pending in the present application. Applicant respectfully requests reconsideration of the present application in view of this response.

Information Disclosure Statement (IDS)

Applicant respectfully submits that the IDS submitted on April 9, 2001 to the U.S. Patent Office was proper in its submission. Applicant understood that the International Application and references cited by the International Searching Authority were sent to the U.S. Patent Office (along with all priority documents et al.). Applicant notes that the Patent Office acknowledges receipt of all documents. Nonetheless, to facilitate the prosecution of this application, Applicant will refile that portion of the IDS that has not yet been considered. Applicant thanks the Examiner for noting the missing documents from the International Searching Authority.

35 U.S.C. § 102(b) – Fiat reference

Claims 4 and 5 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,592,552 to Amos Fiat. ("Fiat reference").

The Fiat reference purportedly concerns a selective broadcasting method operative to transmit a plurality of message data signals to a corresponding plurality of subscriber subsets within a set of subscribers. The method is recited to involve receiving an indication of a privileged set comprising an individual subset and transmitting a message data signal from which a key can be extracted by members of the privileged set and cannot be extracted by any set of members outside the privileged set whose number of members is less than a predetermined resiliency. Further, the Fiat reference refers to length of the message data signal is less than the sum of lengths of the message data signals required if an individual message data signal is transmitted to each subscriber in the privileged set.

To anticipate under 35 U.S.C. § 102, the Patent Office must demonstrate that **each and every claim feature is identically described** or contained in a single prior art reference. See *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 18 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 1991). Here, this is not the case. Claim 4 of the present invention is directed to a process for establishing a common cryptographic key for n subscribers using the Diffie-Hellman process, requiring assigning the n subscribers respective leaves of a binary-structured tree which has a root, n leaves, is of depth [$\log_2 n$] and has treenodes; for each one of the n subscribers, generating a respective secret, the respective secret being assigned to the one of the n leaves to which the one of the n subscribers is assigned; and establishing secrets consecutively in a direction of the root of the tree for all k nodes of the tree starting from the n leaves of the tree across an entire hierarchy of the tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common secret being allocated to a common node so that a common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of the tree.

The Fiat reference does not identically describe each and every claim feature, including the features of: A process for establishing a common cryptographic key for n subscribers using the Diffie-Hellman process, comprising: for each one of the n subscribers, generating a respective secret, *the respective secret being assigned to the one of the n leaves to which the one of the n subscribers is assigned*; and *establishing secrets consecutively in a direction of the root of the tree for all k nodes of the tree starting from the n leaves* of the tree across an entire hierarchy of the tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, *the new common secret being allocated to a common node so that a common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of the tree*, as in claim 4. Instead, the Fiat reference at col. 12 appears to address a method providing each subscriber I with a key, g to the power p_i, where g is a high index value unknown to the subscribers and wherein p_i values are selected such that for any two subscribers i and j, p_i and p_j are relatively prime; providing a message data signal; and encrypting the message data signal using a key which is the modulo N value of g to the power of the product of the p_i values of all subscribers i belonging to the privileged set, where N is a random hard to factor prime composite which is known to the subscribers; and broadcasting a data signal comprising the encrypted message. Fiat reference, col. 12, lines 35-58. The present invention is directed to a process wherein a group key is established with the aid of a tree structure in such a manner so that even after the group key has been established, subscribers can be removed from or added to the key directory without great effort. See Specification.

Accordingly, Applicant respectfully submits that claim 4 is allowable; and respectfully requests withdrawal of the rejection of claim 4 and its dependent claim 5 under 35 U.S.C. § 102(e) over the Fiat reference.

35 U.S.C. § 103(a) – Fiat and Schwenk references

Claim 6 was rejected under 35 U.S.C. § 103(a) over the Fiat reference in view of U.S. Patent No. 6,222,923 to Schwenk ("Schwenk reference").

As discussed above, each and every feature of claim 4 and thus its dependent claim 6 is not described by the Fiat reference and thus is allowable over the Fiat reference. In addition, claim 6 involves the additional features of excluding a selected one of the n subscribers from the tree, the excluding steps including: removing a first one of the n leaves of the tree to which the selected one of the n subscribers is assigned; removing a second one of the n leaves, the second one of the n leaves sharing a common node with the first one of the n leaves, the common node with the first one of the n leaves becoming a new leaf assigned to the one of the n subscribers to which the second one of the n leaves is assigned; and starting from the new leaf of the tree in a direction of the root of the tree, establishing new secrets only in those of the tree nodes which lie within a framework of the tree on a path from the new leaf to the tree root.

The Fiat reference in combination with the Schwenk reference, if such combination were proper (as it is respectfully submitted that it is not), does not disclose or suggest each of the features claimed in claim 6.

The Schwenk reference does not cure the deficiencies of the Fiat reference. The Schwenk reference recites that it is a method for securing a system protected by a predefined hierarchy of cryptographic keys, and in particular, for securing a pay TV system, against unauthorized users. Abstract. In this reference, an individual cryptographic key assigned to a dishonest customer is determined by forming the intersection of at least two predefined subsets formed at different points in time and pertaining to the same hierarchical level. Abstract.

Accordingly, Applicant respectfully submits that claim 6 is allowable, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 103(a) of those claims.

In summary, it is respectfully submitted that all of claims 4 to 6 of the present application are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that rejections of the claims have been overcome. Accordingly, it is respectfully submitted that all claims 4 to 6 are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

If it would further allowance of the present application, the Examiner is invited to contact the undersigned at the contact information given below.

Reg No 47084

Respectfully submitted,

Dated: January 26, 2005

By: ______________________
Richard L. Mayer
(Reg. No. 22,490)

CUSTOMER NO. 26646

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)